UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,877	08/14/2001	Yehuda Afek	0103376-00003	8704

21125 7590 12/19/2005

NUTTER MCCLENNEN & FISH LLP
WORLD TRADE CENTER WEST
155 SEAPORT BOULEVARD
BOSTON, MA 02210-2604

EXAMINER	
JEAN, FRANTZ B	

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 12/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/929,877	AFEK ET AL.	
	Examiner	Art Unit	
	Frantz B. Jean	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/11,4/14/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This is a first office action in response to application for patent filed on 08/14/01. This application claimed benefit of a provisional application filed on 10/17/00. Claims 1-52 are pending in this application.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 3/11/03 and 4/14/03 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

Claim12 is objected to because of the following informalities: on line 2, "to divert traffic is written" twice.

Claim 46 recites "an filter" on line 4.

Claim 48 recites "element that any of authenticates and verifies a source of traffic". This sentence is not clear.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

Claims 20 and 24 recite the limitation "the handshake protocol". There is insufficient antecedent basis for this limitation in the claim.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct

from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-52 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-71 of copending Application No. 11/045,001 and claims 1-102 of copending application 10774,169. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims of the instant application are inherent in the claims of application "001" and "169".

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-52 are rejected under 35 U.S.C. 102(e) as being anticipated by Jungck US patent Number 6,829,654B1.

As per claim 1, Jungck teaches a method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network [see col. 26 lines 29-55], the method comprising the steps of A. with a first set of one or more network elements external to the set of one or more potential victims [see elements 602A, 602B, 604A, 604B, the network elememts can be internal or external see col. 27 lines 4-33; the potential victims are 108, 110], diverting [routing 206 or redirecting] to a second set of one or more network elements external to the set of one or more potential victims traffic otherwise destined for the victim [col. 26 lines 35-50; col. 27 lines 34-46; col. 28 lines 21-39; col. 28 line 47 to col. 29 line 10], B. the element(s) of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim [col. 28 lines 40-46; col. 29 lines 22-64].

As per claim 2, Jungck teaches a method according to claim 1, wherein the diverting step includes effecting a path of traffic that differs from a path that traffic would otherwise take to the victim [redirecting; col. 32 lines 58-60; col. 28 lines 21-34].

As per claim 3, Jungck teaches a method according to claim 1, wherein the filtering step includes detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differ from expected volume, the detecting step includes determining

whether any of the traffic pattern and volume varies statistically significantly [DDOS attack; col. 28 line 40 to col. 29 line10].

As per claim 4, Jungck teaches a method according to claim 1, wherein the filtering step includes detecting suspected malicious traffic [malicious program code, viruses and so on ... col. 28 lines 51 et seq].

As per claim 5, Jungck teaches a method according to claim 4, wherein the detecting step includes detecting packets with spoofed source addresses (col. 26 lines 29-50; col. 28 lines 51 et seq].

As per claim 6, Jungck teaches a method according to claim 5, wherein the filtering step includes detecting traffic requiring a selected service from the victim [col. 29 lines 22-64].

As per claim 7, Jungck teaches a method according to claim 6, wherein the filtering step includes discarding traffic not requiring the selected service from the victim [col. 29 lines 22-64].

As per claim 8, Jungck teaches a method according to claim 7, wherein the filtering step includes discarding any of UDP (is a connectionless mode protocol) and ICMP (is an integral part of IP) packet traffic [col. 28 lines 40-46; col. 31 lines 1-20].

As per claim 9, Jungck teaches a method according to claim 1, wherein the first set and second set include zero, one or more network elements in common [col. 27 lines 15-33].

As per claim 10, Jungck teaches a method according to claim 1, comprising operating one or more elements of the first set at points on the network around the set of one or more potential victim [col. 27 line 34 to col. 28 line 39].

As per claim 11, Jungck teaches a method according to claim 10, comprising operating one or more elements of the second set any of adjacent to or external to one or more elements of the first set [col. 27 line 34 to col. 28 line 39].

As per claim 12, Jungck teaches a method according to claim 10, comprising selectively activating one or more elements of the first set to divert traffic to one or more elements of the second set [col. 27 lines 4-51].

As per claim 13, Jungck teaches a method according to claim 12, activating one or more elements of the first sets to divert traffic in response to a distributed denial of service (DDoS) attack, or notification thereof [col. 28 lines 47 et seq].

As per claim 14, Jungck teaches a method according to claim 12, comprising selectively activating the one or more elements of the first set by any of (i) declaring a network

address of the victim to be close in network distance to one or more elements of the second set, and (ii) declaring the network address of the victim to be far from the victim col. 13 lines 1-19; col. 15 lines 7-37; col. 20 line 65 to col. 21 line 11].

As per claim Jungck teaches 15, a method according to claim 12, comprising associating victim with first and second addresses, and wherein the filtering step includes discarding traffic received external to an area defined by the points directed to the first address, and passing traffic to the victim traffic received external to an area directed to the second address [col. 27 lines 34-51; col 28 lines 21-39].

16. A method according to claim 10, wherein the diverting steps includes redirecting traffic using Policy Based Routing [col. 27 line 13].

As per claims 17 and 21, Jungck teaches a method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of A. with a first set of one or more elements external to the set of one or more potential victims [see elements 602A, 602B, 604A, 604B, the network elememts can be internal or external see col. 27 lines 4-33; the potential victims are 108, 110], diverting [routing 206] to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim col. 26 lines 35-50; col. 27 lines 34-46; col. 28 lines 21-39; col. 28 line 47 to col. 29 line 10], B. the element(s) of the second set filtering traffic diverted in step A

("diverted traffic") and selectively passing a portion thereof to the victim [col. 28 lines 40-46; col. 29 lines 22-64], C. the filtering step including detecting packets with spoofed source addresses by at least partially processing diverted traffic before selectively passing it, if at all, to the victim [diverted traffic can be processed partially as received or fully; col. 28 lines 47 et seq].

As per claims 18 and 22, Jungck teaches a method according to claim 17, wherein the step of at least partially processing diverted traffic includes executing a verification protocol [once traffic is intercepted, verification is performed to determine certain criteria related to the data and its destination; col. 28 lines 47 et seq].

As per claims 19 and 23, Jungck teaches a method according to claim 18, wherein the step of at least partially processing diverted traffic includes executing a TCP three-way handshake with a source of diverted traffic [col. 18 lines 28-67].

As per claims 20 and 24, Jungck teaches a method according to claim 18, wherein the passing step includes passing to the victim traffic from a source that correctly complies with the handshake protocol [col. 18 lines 28-67; col. 27 lines 4 et seq].

As per claim 25, Jungck teaches a method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims [col. 26 lines 32 et seq], the method comprising the steps of A. with a first set of one or more elements

external to the set of one or more potential victims [see elements 602A, 602B, 604A, 604B, the network elememts can be internal or external see col. 27 lines 4-33; the potential victims are 108, 110], diverting [routing 206] to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim [col. 26 lines 35-50; col. 27 lines 34-46; col. 28 lines 21-39; col. 28 line 47 to col. 29 line 10], B. the element(s) of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim [col. 28 lines 40-46; col. 29 lines 22-64, C. the filtering step including discarding [isolating] traffic of selected type [col. 27 lines 34 et seq; col. 28 lines 40 et seq].

26. A method according to claim 25, wherein the filtering step includes discarding any of UDP (is a connectionless mode protocol) and ICMP (is an integral part of IP) packet traffic [col. 28 lines 40-46; col. 31 lines 1-20.

As per claim 27, Jungck teaches a method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of A. with a first set of one or more elements external to the set of one or more potential victims, performing a first filtering of traffic destined for the victim victims [see elements 602A, 602B, 604A, 604B, the network elememts can be internal or external see col. 27 lines 4-33; the potential victims are 108, 110] and diverting [routing 206 or redirecting] to a second set of one or more elements external to the set of one or more potential victims at least a portion of that traffic [col. 26 lines 35-50; col.

27 lines 34-46; col. 28 lines 21-39; col. 28 line 47 to col. 29 line 10], B. the element(s) of the second set performing a second filtering of traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim [col. 28 lines 40-46; col. 29 lines 22-64].

As per claim 28, Jungck teaches a method according to claim 27, wherein the first filtering step includes checking an address of traffic against a network interface through which it is received [col. 29 lines 22-64].

As per claim 29, Jungck teaches a method according to claim 28, comprising tracking changes in traffic paths [col. 29 lines 22-64].

As per claim 30, Jungck teaches a method according to claim 29, comprising sampling traffic that arrives on network interfaces [col. 29 lines 22-64].

As per claim 31, Jungck teaches a method according to claim 29, comprising querying apparent sources of traffic to validate legitimacy [col. 29 lines 38-64].

As per claim 32, Jungck teaches a method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of A. with a first set of one or more elements external to the set of one or more potential victims [see elements 602A, 602B, 604A, 604B, the network

elememts can be internal or external see col. 27 lines 4-33; the potential victims are 108, 110], diverting [routing 206 or redirecting] to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim [col. 26 lines 35-50; col. 27 lines 34-46; col. 28 lines 21-39; col. 28 line 47 to col. 29 line 10], B. the element(s) of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim [col. 28 lines 40-46; col. 29 lines 22-64, C. the filtering step including identifying any of a source and a type of the overload condition [col. 28 line 47 to col. 29 line 10].

As per claim 33, Jungck teaches a method according to claim 32, wherein the identifying step includes statistically measuring [investigating] any of the traffic pattern and volume [col. 28 line 47 to col. 29 line 10].

As per claim 34, Jungck teaches a method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims, the method comprising the steps of A. with a first set of one or more elements external to the set of one or more potential victims [see elements 602A, 602B, 604A, 604B, the network elememts can be internal or external see col. 27 lines 4-33; the potential victims are 108, 110], diverting [routing 206 or redirecting] to a second set of one or more elements external to the set of one or more potential victims traffic otherwise destined for the victim [col. 26 lines 35-50; col. 27 lines 34-46; col. 28 lines 21-39; col. 28 line 47 to col. 29 line 10], B. the element(s) of the second set filtering traffic diverted in step A

("diverted traffic") and selectively passing a portion thereof to the victim [col. 28 lines 40-46; col. 29 lines 22-64, C. the filtering step including detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differ from expected volume [col. 28 line 47 to col. 29 line 10].

As per claim 35, Jungck teaches a method according to claim 34, comprising determining any of a traffic pattern and volume during a period when the victim is not at an overload condition [col. 29 lines 22-64].

As per claim 36, Jungck teaches a method according to claim 35, wherein the determining step includes at least one of analyzing any of netflow data, server logs, victim traffic, and victim volume, and classifying any of traffic pattern and volume according to types of users that generated it [col. 29 lines 22-64].

As per claim 37, Jungck teaches a method according to claim 36, wherein the types of users include individuals users, users sharing a host or proxy, web crawlers and monitoring services [any type of users; col. 27 lines 4-10].

As per claim 38, Jungck teaches a method according to claim 35, wherein the detecting step includes comparing any of a traffic pattern and volume when the victim is at an overload condition with a respective one of a traffic pattern and volume during a period when the victim is not at an overload condition [col. 29 lines 22-64].

As per claim 39, Jungck teaches a method according to claim 38, wherein the comparing step includes determining whether any of the traffic pattern and volume varies statistically with respect to an expected traffic pattern and volume, respectively [Jungck packet's investigation includes the above features; see col. 28 line 47 to col. 29 line 64].

As per claim 40, Jungck teaches a method according to claim 36, wherein the comparing step includes comparing any of traffic volume, port number distribution, periodicity of requests, packet properties, IP geography, and distribution of packet arrival/size [Jungck packet's investigation includes the above features; see col. 28 line 47 to col. 29 line 64].

As per claim 41, Jungck teaches a method according to claim 34, wherein the detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly [Jungck packet's investigation and hackers' detection include the above features; see col. 28 line 47 to col. 29 line 64].

As per claim 42, Jungck teaches a method according to claim 34, wherein the detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly from any of an expected pattern and volume, respectively significantly [Jungck packet's investigation and hackers' detection include the above

features; see col. 28 line 47 to col. 29 line 64].

As per claim 43, Jungck teaches a method according to claim 42, comprising determining any of a traffic pattern and volume during a period when the victim is not at an overload condition [col. 29 lines 22-64].

As per claim 44, Jungck teaches a method according to claim 43, wherein the determining step includes analyzing any of netflow data, server logs, victim traffic, and victim volume [col. 29 lines 22-64].

As per claim 45, Jungck teaches a method according to claim 44, wherein any of the determining steps include classifying any of traffic pattern and volume according to types of users that generated it [col. 28 line 62 to col. 29 line 64].

As per claim 46, Jungck teaches a network element [602] for use in protecting against an overload condition on a network, the network element comprising: an input for receiving traffic from the network [col. 27 lines 34-46; and 9-19]; an filter [606] coupled to the input, the filter selectively blocking traffic originating from a source suspected as potentially causing the overload condition, a statistics module that is coupled to the filter and that identifies traffic statistically indicative of having originated from source potentially causing the overload condition, and an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter

[col. 29 lines 22-64; col. 28 line 40 to col. 29 line 10].

As per claim 47, Jungck teaches a network element according to claim 46, comprising a termination detection module that at least participates in determining when the overload condition has ended [col. 28 line 47 to col. 29 line 10].

As per claim 48, Jungck teaches a network element according to claim 46, comprising an antispoofing element that any of authenticates and verifies a source of traffic [col. 28 line 47 to col 29 line 64].

As per claim 49, Jungck teaches a system for use in protecting against an overload condition on a network, the network element comprising: one or more network elements ("guards") [602A, 602B] disposed on the network, each network element having an input for receiving traffic from the network, an filter [606] coupled to the input, the filter selectively blocking traffic originating from a source suspected as potentially causing the overload condition, a statistics module that is coupled to the filter and that identifies traffic statistically indicative of having originated from a source suspected as potentially causing the overload condition [col. 27 lines 4-46; col. 29 lines 22-64], and an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter, one or more further network elements ("diverters") disposed on the network and in communication with the guards, the further network elements selectively (i) diverting to one or more guards traffic otherwise destined for a still further

network element ("victim") in a set of one or more potential victims on the network [col. 27 lines 4-46; col. 29 lines 22-64] .

As per claim 50, Jungck teaches a system according to claim 49, wherein one or more guards comprises a termination detection module that at least participates in determining when the overload condition has ended [col. 28 line 47 to col. 29 line 10].

As per claim 51, Jungck teaches a system according to claim 49, wherein one or more guards comprises an ingress filter, coupled to the statistical module, that generates and transmits to a further network element on the network rules for blocking traffic on the network [col. 29 lines 11-64].

As per claim 52, Jungck teaches a network element according to claim 49, comprising an antispoofing element that any of authenticates and verifies a source of traffic [col. 28 line 47 to col 29 line 64].

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Shawcross US patent 6,880,090 B1 discloses a method and system for IP network communications and a use for protecting Internet sites against DDOS attacks on insecure public networks.

This reference discloses limitations that are relevant to the claimed invention. Applicant is requested to consider this prior art of record upon responding to this office action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Frantz B. Jean whose telephone number is 571-272-3937. The examiner can normally be reached on 8:30-6:00 M-f.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung can be reached on 571 272 3939. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

FRANTZ B. JEAN
PRIMARY EXAMINER

Frantz Jean